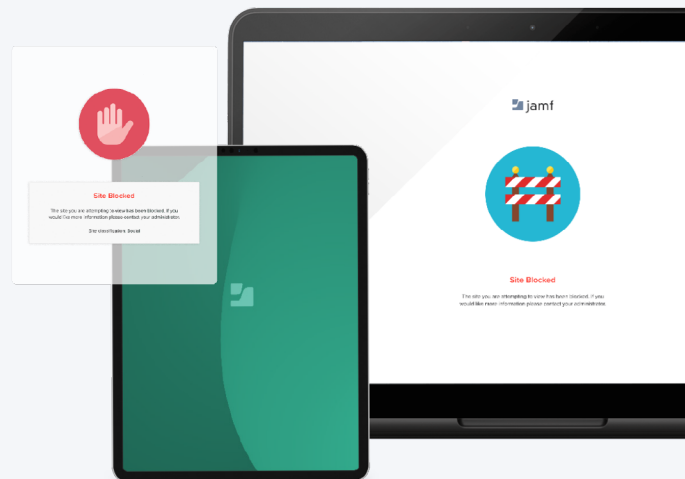




Overal waar geleerd wordt veilige privé verbindingen



Jamf Safe Internet op basis van de engine voor contentfiltering en bescherming tegen netwerkbedreigingen van Jamf is ontwikkeld om scholen te helpen hun leerlingen, personeel en netwerken te beschermen tegen schadelijke content.

Leerlingen brengen bijna twee keer zoveel tijd online door als voorheen. Dat betekent dat er een groeiende behoefte is aan digitale veiligheid om cyberaanvallen uit te sluiten en te voorkomen dat leerlingen toegang krijgen tot onveilige content.

Jamf Safe Internet is speciaal ontwikkeld voor onderwijs, contentfiltering en beveiliging met beveiligingstools van Jamf. De oplossing combineert de beste preventie van netwerkbedreigingen en een zeer uitgebreide database van contentfilters om onveilige content en kwaadaardige aanvallen zoals malware of phishing te blokkeren. Bovendien is het geïntegreerd met ons paradepaardje voor het beheer van mobiele apparaten voor het onderwijs: Jamf School.

Cyberbeveiliging die altijd aan staat

In het onderwijs is het essentieel dat netwerken tegen cyberaanvallen worden beschermd, om de continuïteit van het onderwijs te waarborgen, gegevens van personeel en leerlingen te beschermen en andere potentiële risico's die met deze aanvallen gepaard gaan, te elimineren.

Bedreigingspreventie en filtering op het apparaat

Verbeter de beveiliging op apparaatniveau. De eerste beveiligingsscan en contentfilterinspectie vinden plaats op het apparaat, waardoor je gebruikers en je organisatie een veiligere, proactieve ervaring hebben. *(Exclusief voor Apple)*

Contentfiltering

Beperkingen afdwingen

Gebruik Jamf Safe Internet om de beperkte modus van YouTube te implementeren en Google SafeSearch af te dwingen. Verberg expliciete content van zoekopdrachten en opmerkingen, en ingesloten YouTube-video's op YouTube en in Google-zoekresultaten.

Database voor contentfilters

Uitgebreide contentfiltering geoptimaliseerd voor het onderwijs en geïntegreerd met MDM voor eenvoudige, krachtige bescherming van gebruikers. Met behulp van lichtgewicht, hoogwaardige domeinnaamsysteem (DNS)-technologie stelt Jamf Safe Internet beheerders in staat om de contentfilterresultaten te creëren en aan te passen aan hun schoolbehoeften, zonder inbreuk te maken op de privacy.

Beleidsschema's

Pas strenge controles toe tijdens de lestijden en laat meer flexibiliteit toe wanneer de apparaten thuis zijn. Met een tijdgebaseerd beleid is er gemakkelijk een balans te vinden tussen veiligheid, naleving en keuzevrijheid van de ouders.

Preventie van bedreigingen

Beveiliging tegen malware, phishing en cryptojacking

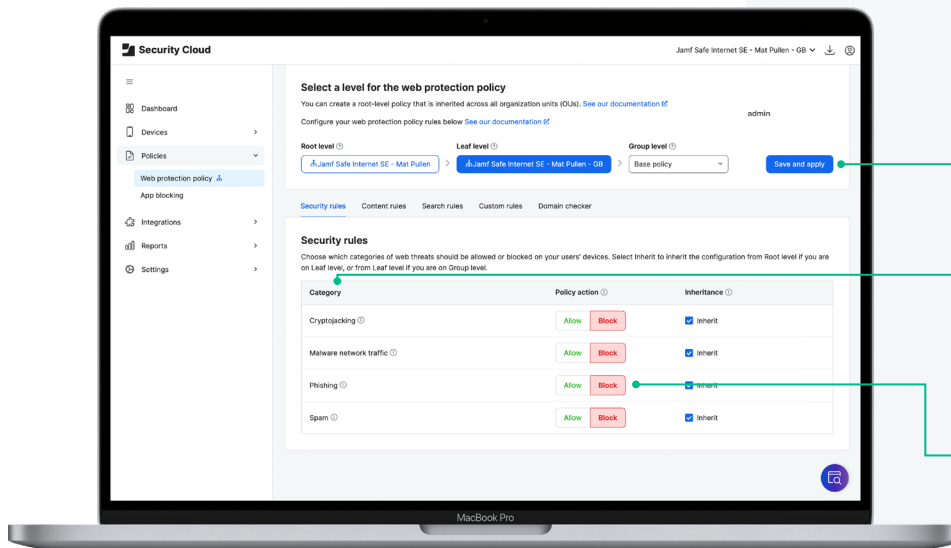
Jamf Safe Internet maakt gebruik van machine learning tools om phishing, malware, cryptojacking en andere vormen van cyberaanvallen te identificeren en te bestrijden, zodat instellingen en hun netwerken veilig blijven.

Privacygericht, flexibel ontworpen

De privacygerichte benadering van Jamf past zich aan elke implementatie aan. IT regelt de zichtbaarheids- en beschermingsniveaus, waarmee de leerlingen en de gegevensprivacy beschermd zijn en de leerprocessen zonder onderbrekingen kunnen doorgaan.

Aangepaste contentcontroles

Bepaal het beveiligings- en filterbeleid dat past bij jouw behoeften. Of kies een van de voorinstellingen van Safe Internet en ga meteen aan de slag!



Eenvoudig updates van jouw beleid opslaan en toepassen

Brede reeks blokcategorieën om bepaalde content te voorkomen

Eenvoudige click-to-toggle-functie voor toestaan/blokken

Zie hoe **Jamf Safe Internet** er samen met jouw MDM-platform voor zorgt dat beveiliging en digitale veiligheid centraal in de educatieve ervaring blijven staan.



www.jamf.com/nl

© 2025 Jamf, LLC. Alle rechten voorbehouden.

Ga naar jamf.com/nl om te zien hoe Jamf Safe Internet leerlingen en gebruikers beschermt.